UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	HOPKINS et al.	Docket No: 20206-16 (P00-3324)
Serial No:	Not Yet Assigned	Group Art Unit: Not Yet Assigned
Filed:	Herewith	Examiner: Not Yet Assigned

For: **MULTIPLE PRIME NUMBER GENERATION USING A PARALLEL PRIME NUMBER SEARCH ALGORITHM**

Box New Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL FOR INFORMATION DISCLOSURE STATEMENT

Enclosed for filing in the above-identified application is an Information Disclosure Statement with attached Form PTO-1449 and copies of cited references.

The Commissioner is authorized to charge any required fees, or credit any overpayment to Deposit Account No. 02-3964 (Order No. 20206-16(P00-3324).

Respectfully submitted,

DATE: 3|26|2001

Justin Boyce
Reg. No. 40,920

OPPENHEIMER WOLFF & DONNELLY LLP
Customer No. 25696
1400 Page Mill Road
Palo Alto, CA 94043
Tel. No: (650) 320-3000
Fax. No: (650)320-3100

CERTIFICATE OF MAILING (37 CFR 1.10(A))
CERTIFICATE OF MAILING BY "EXPRESS MAIL" - Rule 10: I hereby certify that this correspondence is being deposited with the U. S. Postal Service "Express Mail Post Office to Addressee" under 37 CFR 1.10 as Express Mail No. EL654883265US addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231 on March 26, 2001 by Elizabeth Kim.

Date: March 26, 2001

Elizabeth Kim

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY DOCKET NO. 20206-16 (P00-3324)	SERIAL NO. Not Yet Assigned	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	APPLICANT HOPKINS, et al.		
	FILING DATE Herewith	GROUP Not Yet Assigned	

U. S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA	4,168,396	09/18/1979	Best	178	22	10/31/1977
	AB	4,200,770	04/29/1980	Hellman, et al.	178	22	09/06/1977
	AC	4,218,582	08/19/1980	Hellman, et al.	178	22	10/06/1977
	AD	4,278,837	07/14/1981	Best	178	22.09	06/04/1979
	AE	4,405,829	09/20/1983	Rivest, et al.	178	22.1	12/14/1977
	AF	4,424,414	06/03/1984	Hellman, et al.	178	22	05/01/1978
	AG	4,319,079	03/09/1982	Best	178	22.09	01/17/1980
	AH	4,433,207	02/21/1984	Best	178	22.09	09/10/1981
	AI	4,465,901	08/14/1984	Best	178	22.08	07/02/1981
	AJ	4,514,592	04/30/1985	Miyaguchi	178	22.11	07/14/1982
	AK	4,995,082	02/19/1991	Schnorr	380	23	02/23/1990
	AL	5,046,094	09/03/1991	Kawamura, et al.	380	46	02/02/1990
	AM	5,321,752	06/14/1994	Iwamura, et al.	380	24	09/04/1992
	AN	5,343,527	08/30/1994	Moore	380	4	10/27/1993
	AO	5,351,298	09/27/1994	Smith	380	30	09/30/1992
	AP	5,421,006	05/30/1995	Jablon, et al.	395	575	04/20/1994
	AQ	5,761,310	06/02/1998	Naciri	380	30	07/18/1996
	AR	5,835,594	11/10/1998	Albrecht, et al.	380	23	02/09/1996
	AS	5,844,986	12/01/1998	Davis	380	4	09/30/1996

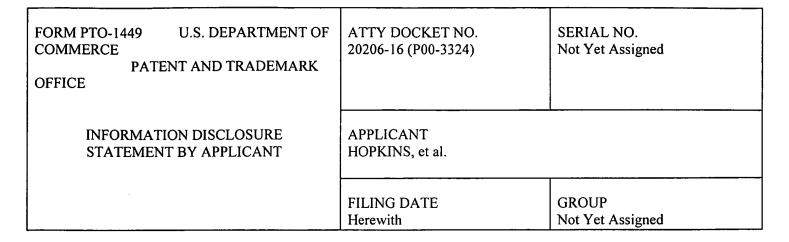| FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY DOCKET NO. 20206-16 (P00-3324)	SERIAL NO. Not Yet Assigned
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	APPLICANT HOPKINS, et al.	
	FILING DATE Herewith	GROUP Not Yet Assigned

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	NAME	CLASS	SUBCLASS	TRANSLATION YES NO
	AT							

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	AU /	S.A. VANSTONE et al., "Using Four-Prime RSA in Which Some of the Bits are Specified," December 8, 1994, Electronics Letter, Vol. 30, No. 25. pp. 2118-2119
	AV /	C. COUVRUER et al., "An Introduction to Fast Generation of Large Prime Numbers," 1982, Philips Journal of Research, Vol. 37, Nos. 5-6, pp. 231-264.
	AW /	Y. DESMEDT et al., "Public-Key Systems Based on the Difficulty of Tampering (Is There a Difference Between DES and RSA?)," 1986, Lecture Notes in Computer Science, Advances in Cryptology-CRYPTO '86 Proceedings.
	AX /	J. J. QUISQUATER et al., "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem" October 1982, Electronic Letters, Vol. 19, No. 21.
	AY /	CETIN KAYA KOC, "High-Speed RSA Implementation (Version 2.0)," November 1994, RSA White Paper, RSA Laboratories.
	AZ /	RIVEST et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," February 1978, Communications of the ACM, Vol. 21.
	BA. /	PKCS #1: RSA Encryption Standard (Version 1.5), November 1993, RSA Laboratories Technical Note.
	BB. /	M.O. RABIN, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization," January, 1979, MIT Laboratory for Computer Science.
	BC. /	R. LIDL et al., "Permutation Polynomials in RSA-Cryptosystems," 1984, Advances in Cryptology—Crypto '83, pp. 293-301.
	BD. /	D. BONEH et al., "Generating a Product of Three Primes with an Unknown Factorization," Computer Science Department, Stanford University.
	BE. /	J. J. QUISQUATER et al., "Fast Generation of Large Prime Numbers" June 1982, Library of Congress, Catalog No. 72-179437, IEEE Catalog No. 82CH1767-3 IT, pp. 114-115
	BF. /	A. J. MENEZES et al., "Handbook of Applied Cryptography", 1997, Library of Congress catalog No. 96-27609, pp. 89, 612-613

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY DOCKET NO. 20206-16 (P00-3324)	SERIAL NO. Not Yet Assigned
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	APPLICANT HOPKINS, et al.	
	FILING DATE Herewith	GROUP Not Yet Assigned

	BG.	P.J. FLINN et al., "Using the RSA Algoithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify Without Infringing the RSA Patent?", July 9, 1997, 17 pgs, http://www.cyberlaw.com/rsa.html
	BH.	NEMO, "RSA Moduli Should Have 3 Prime Factors", 1996

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.